STRATEGY RESEARCH PROJECT



# INFORMATION WARFARE AND THE LACK OF A U.S. NATIONAL POLICY

BY

LIEUTENANT COLONEL ROBERT H. WHISENHUNT
United States Army





USAWC CLASS OF 1996


U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGIC RESEARCH PROJECT



# INFORMATION WARFARE AND THE LACK OF A U.S. NATIONAL POLICY

by

Lieutenant Colonel Robert H. Whisenhunt
United States Army

Lieutenant Colonel James O. Kievit
Project Advisor

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: Robert H. Whisenhunt (LTC), USA

TITLE: Information Warfare and the Lack of a U.S. National Policy

FORMAT: Strategic Research Project

DATE: 15 April 1996 PAGES: 27 CLASSIFICATION: Unclassified

The information technology explosion is having a profound impact on the Information Infrastructure of the United States. This has led to growing national security problems for government agencies as well as private industry. The problems are not totally new, but the speed at which technology allows information processes to take place has raised their relative importance in the conduct of daily commerce. The greatest return on investment appears to be in the area of improved defensive capabilities of our networks. Many agencies and departments (government and private industry) are working on the problem independently. Cooperation and coordination are either unlikely or will take far too long. The best approach is a policy statement from the Executive Branch that places the responsibility on a single agency or committee to integrate these fragmented efforts into a coherent program for national security.

## Introduction

Information Warfare is not new. It has been practiced throughout history under a multitude of identifiers. Whether you call it communications, misinformation, disinformation, deception, or any of a long list of names, the use of information to gain an advantage is as old as conflict itself. In the Information Age, we are harnessing technology which allows us to collect, process, and distribute information at an ever increasing rate. This increased speed and capability has turned the use of information into a major force multiplier of increasing importance.

Information and information systems are becoming more commonplace in our everyday society. Our dependence on information is growing. The tools that help us automate the decision processes are available from multiple sources. This has opened up our national information infrastructure to anyone who wishes to use it. While the U.S. government, and in particular the Department of Defense, is currently working on future concepts for the employment of technological developments, they have not invested the necessary resources to secure the current systems from which these future systems may evolve. Defense against attacks on our information systems is a growing national security problem, which will not be solved without an executive decision on what is to be done and who is in charge.

## The Information Warfare Problem

The rapid advances in information technologies are creating new problems and vulnerabilities for agencies of the United

States government. Digital data can be manipulated, corrupted, or even deleted from great distances. Direct Broadcast Satellite systems can provide a video conduit to a target audience for the purposes of propaganda campaigns. He who controls information controls the views and opinions of the people and ultimately shapes the political will of the nation. National information systems will become the targets of the next war. In fact, the National Information Infrastructure may become the de facto "center of gravity"[1] for future conflict.

It is vitally important that the United States develop a coherent strategy against attacks on its vital information systems. Some pieces of this strategy are currently in place, but they are fragmented and there is no overarching directive from the Executive Branch which could serve as National Policy. We do not have a coordinated program or capability to protect our national information systems. We do not even have an accepted single definition of what constitutes Information Warfare. The lack of a concerted effort to develop a program or strategy has not been the result of indifference or ambivalence. In fact, our national leaders are very aware of the tremendous power which information technology brings to the face of war. Secretary of Defense William Perry said on May 5, 1994:

> "We live in an age that is driven by information.... The ability to acquire and communicate huge volumes of information in real time, the computing power to analyze this information quickly, and the control systems to pass this analysis to multiple users simultaneously -- these are the technological breakthroughs that are changing the face of war and how we prepare for war."[2]

And our military leaders are recognizing that we cannot continue to subscribe to war in the old paradigms of force-on-force ratios, taking and holding terrain, and attacking deep through air and naval superiority. As General Ronald R. Fogelman, Air Force Chief of Staff, puts it:

> "If you use as your starting point the beginning of the 20th Century, you recognize that war had been fought in two dimensions - on land and at sea. Then, with the airplane, warfare took on a third, vertical dimension....I think the next major advance came in the Space Age. This is the fourth dimension of warfare....I will also tell you that [the] information explosion I mentioned signals that we are crossing a new frontier. Information has an ascending and transcending influence -- for our society and our military forces. As such, I think it is appropriate to call information operations [warfare] the fifth dimension of warfare. Dominating this information spectrum is going to be critical to military success in the future."[3]

If the United States is to maintain its technological superiority and dominate the information warfare environment, we must begin to approach this problem with a new awareness. Information Warfare is a new way of doing business; a new war-fighting discipline that must be incorporated into doctrine, training, and materiel acquisition programs at all levels if we are to achieve success on the future battlefield. In the past, technology innovation and breakthroughs were realized in government laboratories or under the cognizance of government contracts. When it was deemed appropriate, the technology was provided to private industry for adaptation to commercial products. Today, the reverse is true. More and more, the defense laboratories are being dismantled by budgetary cuts and

private industry is conducting more research and development in the areas of advanced technologies. The Department of Defense is moving in a new direction of incorporating dual use technology programs of commercial research and development departments with only a limited number of Defense Department labs remaining active. These commercial vendors can provide for many of our needs at less cost than we can research and develop it ourselves. This is most prevalent in the way DoD satisfies its current world-wide communications requirements.

> "The national security posture of the United States is depending more and more on the U.S. information infrastructure and the larger global information infrastructure (GII). These information infrastructures (which consist of information, information systems, telecommunications, networks and technology) depend, in turn, upon other infrastructures such as electrical power and energy. Over 95 percent of the worldwide telecommunications needs of the Department of Defense are satisfied by commercial telecommunications carriers."[4]

This increased dependency on commercial service providers comes as a double-edged sword. While state of the art technologies can be rapidly incorporated into the military's information infrastructure, these same commercial systems bring inherent dangers via increased vulnerabilities to information technology attacks. The nature of technological advances is outpacing defensive capabilities. The decreasing costs of these technologies make them affordable in small quantities. And these small quantities may be all that is necessary to disrupt or paralyze our information networks for governmental operations, banking, transportation or public utilities. While we continue

to focus our efforts on future concepts, we cannot continue to perpetuate the current state of our infrastructure defenses. Noted authors, governmental agencies, and members of Congress share a common concern that we are not doing enough to protect the current infrastructure from attack. Winn Schwartau of Inter-Pact notes,

> "With over 100 million computers inextricably tying us all together through the most complex array of land and satellite based communications systems...government and commercial computer systems are so poorly protected today that they can be essentially considered defenseless. An electronic Pearl Harbor is waiting to happen."[5]

Alan D. Campden, author of The First Information War, supports this view when he says, "No nation is more vulnerable than the United States to electronic attacks, nor, apparently more reluctant to confront this potentially disabling weakness."[6] The security of our military information systems is not immune to these electronic attacks. Douglas Waller of Time magazine notes,

> "While the military's actual war-fighting computers are generally deemed secure, those supporting other vital areas - such as payroll, personnel, transportation and spare parts - are handled by poorly guarded Pentagon computers linked by scantily protected public-communications channels."[7]

The service chiefs are also recognizing this increased vulnerability of their forces. The Defense Information Systems Agency (DISA) has developed teams of professionals to assess network vulnerabilities within the DoD. The objectives of these teams are to identify system vulnerabilities, devise countermeasures, support infrastructure improvement, and raise awareness of threats to system integrity, availability, and

confidentiality. More than 16,000 DoD host computers were "attacked" by these teams. Here are some of the results:

> " - 3.3% of DoD tested computers have exploitable front doors.
> - 88% of DoD tested computers were penetrated using network trust relationships.
> - 96% of the penetrations were never detected by host administrators or users.
> - 95% of the penetrations detected went unreported."[8]

The Navy's Fleet Information Warfare Center (FIWC) has a similar capability and conducted similar tests on its own network with the same discouraging results. So even with a heightened awareness focused on information security, the DoD is still incredibly vulnerable. This does not bode well for many other agencies within government and the civilian sector. In fact,

> "Outside the military, The National Security Agency is deeply worried that computers controlling banking, stock exchanges, air-traffic control, phones, and electrical power could easily be crippled by determined hackers. 'We're more vulnerable than any other nation on earth,' says NSA director Vice Admiral John McConnell. A wired adversary could take down these computers 'without ever entering the country,' an outside panel studying future Pentagon missions warned in a report last May [95]. The results of such attacks could cause 'widespread fear throughout the civilian population,' according to another Pentagon report released last December [94]."[9]

The only tools a hacker or potential adversary would need to carry out these attacks are a computer, a modem, and a telephone line. With the telephone number to a local (or any) Internet host, the intruder could be electronically teleported to almost anywhere in the world in a matter of a few seconds.

> "Within the last two years, electronic intruders have penetrated major U.S. telecommunications carriers and Internet service providers, many international Post,

> Telegraph, and Telephone [PTT] organizations, and a wide variety of end-user systems. These intruders have included foreign intelligence agents, economic espionage agents, organized crime members, drug cartel members, private detectives, hackers, and insiders."[10]

In view of the apparent fragility associated with these systems, industry must work on improvements to mitigate these vulnerabilities. Better defenses must be engineered if we are to retain the integrity and reliability of our information systems.

Our elected representatives also recognize the need for immediate action.

> "House Speaker Newt Gingrich (R-GA) cautioned an AFCEA conference on information warfare that 'Cyberspace is a free flowing zone to which anyone has access, if they have a minimal level of capital...and we had better be prepared for zones of creativity in our opponents we've never dreamed of.'"[11]

Senator William V. Roth (R-Del), another vocal critic of the current administration's programs in the area of information security, requested a study of security programs by the Office of Technology Assessment (OTA) of the U.S. Congress. In prepared remarks, Senator Roth states,

> "We need to recognize the potential danger [of information vulnerabilities] and act accordingly. Last year [1994], I asked the Office of Technology Assessment to look at such problems and recommend changes. Its report notes that the government is not doing a good job here. The report warns that, '...without careful planning, understanding security concerns, and adequate training, the prospect for plagiarism, fraud, corruption or loss of data, and improper use of networked information could affect the privacy, well-being, and livelihoods of millions of people.'"[12]

In an assessment of the vulnerabilities to the security of our national communications systems, Sen John Kyl (D-N.M.) said,

"There is currently no defense against attacks on our nation's information systems, which include our defense, telephone, public utilities and banking systems."[13]

**Potential Solutions to the Problem**

With consensus that there are vulnerabilities and no existing program for defense of the infrastructure, measures must be taken to minimize our technological exposure. Potential solutions might be found in the areas of legal reform or enactment of laws to regulate the environment, developing a capability or strategy to deter an information attack, launching a pre-emptive strike against a potential aggressor, or increased expenditure of resources to improve our system defenses.

The concept of outlawing information attacks is appealing. However, there are 2 reasons why this approach would not be selected. First, the collection of laws that currently attempt to regulate the area of information security deals with attacks by Americans on American networks or computers, from within the borders of the United States. Examples of these laws include:

> "- I,IV,V,and XIV Amendments to the U.S. Constitution, The Privacy Act of 1974 (Protects personal privacy from invasion by Federal agencies), Foreign Intelligence Surveillance Act of 1978 (Restricts collection of information on U.S. citizens), Electronic Communications Privacy Act of 1986 (Updates Federal privacy provisions incorporating new technologies), Communications Assistance for Law Enforcement Act of 1994 (makes clear telecommunications carriers duties and responsibilities to cooperate with law enforcement), Title XXIX - Computer Crime Amendment to the Violent Crime Control and Law Enforcement Act of 1994 (Defines what constitutes computer crime)."[14]

It is also important to note that punishment can only be exacted

if the entity committing the crime is identified and caught. To the hacker, nation, or any other user, outside the United States, these laws have little, if any, deterrent effect because they simply do not apply in the international community. The National Information Infrastructure is a subset of the Global Information Infrastructure. There are currently no laws, treaties, or agreements that deal with this problem at the international level. It could prove illogical to think the international community could husband a proposal that would lead to the development of a common basis for agreement ensuring the availability, credibility, privacy, and security of our networks in the Information Age. These actions would be encumbered by the fact that any laws, treaties, or agreements would have to be enforceable, and generally accepted as relevant by the community at large.

Secondly, when dealing with cyberspace, and the many who use it from all over the world, it is necessary to note an emerging mindset that may be much different from our own. An example of this can be found in an extract from "A Declaration of the Independence of Cyberspace" by John Perry Barlow, co-founder of the Electronic Frontier Foundation.

> "...Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not come from Cyberspace, the new home of Mind.
>
> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor

> do you possess any methods of enforcement we have true reason to fear.
>
> You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature, and grows by itself through our collective actions."[15]

The author's point that there are no "methods of enforcement" that he has "true reason to fear" demonstrates the difficulty of establishing a legal strategy for defense against information warfare. Not only the lack of laws, be they national or international, but the lack of acceptance of laws on levels different than those of agreeing nation-states, could have a profound impact.

The idea that we can legislate the environment of cyberspace through the enactment of laws might appear a fruitful path, but the inability to enforce these laws will make them totally useless. A universal legal approach will not work. If legal actions would be ineffective, can deterrence be of any appreciable use in the information warfare environment?

To theorize whether or not deterrence is possible, it is necessary to examine deterrence as an art and how deterrence can be developed and used. "Deterrence is the inducement of another party to refrain from a certain action by means of a threat that this action will lead the threatened party to inflict retaliation or punishment."[16] The development of a deterrence strategy often pre-supposes that the identity of the threat or the attacker is known. Our nuclear deterrence strategy was developed against those nations that were known to possess a nuclear capability.

In cyberspace, the threat can emerge from the spectrum of actors who are national or international; rational or irrational; nation-state or individual. Information warfare does not provide the luxury of limiting the scope of our concerns.

A deterrence strategy must also possess the credibility and veracity of the retaliatory capability. Looking again to our nuclear deterrence strategy, our possession of nuclear weapons is a fact, the totally destructive nature of nuclear weapons has been chronicled in numerous test reports, and our previous use of atomic weapons is indisputable. These facts serve as the "inducement" for other nations to refrain from nuclear attacks on the United States because their own interests would not be realized or the price would be too great. Our possession of weapons to prosecute the information war are currently rumors. We have advanced technological capabilities but they have not been demonstrated and the community at large is still unsure about the level of devastation which might be realized from their employment. Because the information infrastructure is so amorphous, any attempt to develop a proactive deterrence capability would be difficult and might very well fail if attempted.

Since acceptable laws may not be universally agreed to within the international community and the nature of the environment makes an effective deterrence strategy implausible, the only recourse is to place greater emphasis on an ability to prevent attacks upon our information systems. This would be

accomplished through the use of pre-emptive strikes against other aggressor information systems or increased defenses of our own systems making penetration much more difficult.

Should the U.S. launch a pre-emptive information attack against the information infrastructure of another sovereign nation, the act could be construed as an overt act of war. Not only would this approach find little political support, but would be patently unethical if not illegal under current U.S. law. The portability of the equipment and the multi-link architecture of the global infrastructure allows any adversary to select multiple locations and different paths for successive attempts on our systems. Not knowing what constitutes an attack, where these attacks are being initiated, or the identity of the individual, group, or nation behind them, makes a pre-emptive attack virtually impossible.

Given the facts that we have had only limited success with outlawing weapons and given the difficulties inherent in deterrence or pre-emptive measures, the best use of our resources would be on programs that develop better defenses for our information systems. This will require an aggressive technology program shared by government and private industry. Both are equally vulnerable to the current situation. Disparate organizations will be forced to combine their knowledge of the problem and develop a coherent integrated approach to resolve the existent vulnerabilities. What is desired by private citizens, private industry and the government is an information network

that is credible, available, secure, and survivable. This will only be achieved through the development of a national policy or program that has the mandated authority to integrate the multiple fragmented efforts that are on-going today.

## Obstacles to Successful Defense

Many governmental agencies, departments, committees, councils and boards have been established to advise, recommend, and propose technological solutions to this issue. Government and the private sector are working together in some quarters to achieve resolution. Each, however, tends to have its own definition of the problem and an equally unique concept for what should be done and by whom.

How are departments and agencies defining or characterizing information warfare? Emmet Paige, Jr., (ASDC3I), defines it this way: "Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information and information systems."[17] This definition specifically limits actions to those in support of our national military strategy. It does not address other critical information systems like the Federal Reserve Banking and the Air Traffic Control systems. The U.S. Air Force uses the following definition; "Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own information functions."[18] While this definition does not limit itself in its

scope, it does identify the actions of an "enemy." This term does not lend itself favorably outside a purely military context. The School of Information Warfare and Strategy defines information warfare as,

> "(1) Aggressive use of information means to achieve national objectives. (2) The sequence of actions undertaken by all sides in a conflict to destroy, degrade, and exploit the information systems of their adversaries. Conversely, information warfare also comprises all actions aimed at protecting information systems against hostile attempts at destruction, degradation, and exploitation. Information warfare actions take place in all phases of conflict evolution: peace, crisis, escalation, war, de-escalation, and post conflict periods."[19]

Again, this definition limits its scope to national objectives. It also defines itself in the military context by describing the phases of conflict. The definition which has been approved for use within the U.S. Army is, "Actions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems, while defending ones own information, information-based processes, and information systems."[20] In reviewing these definitions, it is easy to discern the military mind-set with which they were developed. This should come as no surprise since the Department of Defense has been the major contributor to these efforts for quite some time. Many of these definitions limit themselves to applications within the framework of the military's role in defense of the nation's vital interests. Peculiarly, the Army's definition seems to be more broadly based and could be found acceptable to other than military institutions. This definition

could easily serve as a point of departure for establishing ground truth and a common basis for the exchange of information among other non-military entities who are wrestling with information warfare issues as they relate to our information infrastructure. These efforts remain fragmented with little or no interaction between the various factions working on the same problem. A national policy on information warfare would bring order out of chaos by establishing an accepted definition and assigning responsibilities for merging these fragmented efforts into a coherent program with national objectives and direction.

Congress has enacted legislation which assigns some responsibilities at the macro level, but is deficient in the details. The Department of Defense recognized the lack of assigned responsibilities, and the resultant vulnerabilities. And it is working toward solutions to eliminate them. These technological vulnerabilities are identified in many of our national strategy documents. Our National Security Strategy states, "The threat of intrusions to our military and commercial information systems poses a significant risk to national security and must be addressed."[21] From this document, the Chairman of the Joint Chiefs of Staff prepares the National Military Strategy which states,

> "WIN THE INFORMATION WAR - The remarkable leverage attainable from modern reconnaissance, intelligence collection and analysis, and high-speed data processing and transmission warrants special emphasis. The services and combatant commands require such fused information systems. These systems enhance our ability to dominate warfare. We must assure that this leverage works for us and against our adversaries. New doctrine

> is being developed, and training and control programs are underway, to ensure that advantages, built on the early success in Operation Desert Storm, are being exploited."[22]

For example, the Department of the Army has or will in the very near future publish its doctrinal effort in Information Operations. The new document will be called FM 100-6, Information Operations. This manual "supports battle command and provides guidelines for commanders who will conduct information operations in support of all phases of the force projection operating environment,..."[23]

Other agencies within the Federal government also have responsibilities for our information infrastructures.

> "The Communications Act of 1934 gives OMB [Office of Management and Budget] and Department of Commerce (DoC) roles in executive branch telecommunications. The Federal Property and Administrative Services Act of 1949, the Brooks Act of 1965, and the Paperwork Reduction Act of 1980 give OMB, DoC, National Institute Of Standards and Technology (NIST) and GSA [Government Services Agency] roles in procuring and managing federal information technology....A major factor in the handling of information is the delineation of responsibilities by the Computer Security Act of 1987 for classified and unclassified information. Although DoD has traditionally placed itself at center stage in the on-going debate regarding information handling, the act very clearly assigned responsibility for policy formulation for sensitive unclassified information to the Department of Commerce. The NIST was further delegated the responsibility for sensitive unclassified standards and guidelines. The DoD retained its role for classified information."[24]

The Computer Security Act attempts to bisect the information world into classified and unclassified with no overlap. For those systems the DoD employs on its classified networks there is a standard and guideline developed by the DoD. Yet for its

unclassified but sensitive computer networks, the standard and guidelines to be followed are those developed by the National Institute of Standards and Technology. There must be greater overlap between governmental agencies to achieve consensus on the appropriate direction for future policy considerations. Many of our current guidelines were written some time ago and the information explosion has rendered them antiquated if not obsolete.

> "In May 1993, the Secretary of Defense and the Director of Central Intelligence established a Joint Security Commission (JSC) to examine the processes used to formulate and implement security policy in the DoD and Intelligence Community....The JSC recommended the creation of a joint DoD/DCI security executive committee, and that the committee oversee development of a coherent network-oriented information systems security policy for the Department of Defense and the Intelligence Community that also could serve the entire government."[25]

When the findings and recommendations of the Joint Security Commission were reviewed, it was determined that such a committee was needed. The Executive Branch answered this recommendation with the signing of Presidential Decision Directive (PDD) 29 in late 1994, establishing the Security Policy Board. The charter of this new board was to "consider, coordinate, and recommend for implementation to the President, through the Assistant to the President for National Security Affairs, policy directives for U.S. security policies, procedures and practices."[26] Recognizing the need to include civilian and non-governmental agencies in the formulation of policy recommendations, "PDD 29 also established the Security Policy Advisory Board to provide a non-governmental

and public perspective on security policy initiatives."[27] It should be noted that these boards are "advisory" and are therefore only in a position to advise and recommend versus establish national policy. Another group that is actively pursuing the information infrastructure issue is the President's National Security Telecommunications Advisory Committee (NSTAC).

> "The President created the NSTAC by Executive Order 12382 in September 1982 to advise him on matters regarding national security and emergency preparedness telecommunications....The NSTAC has been validated biennially, most recently by Executive Order 12974, 29 SEP 1995. Membership is limited to 30 presidentially appointed industry leaders. Currently, the NSTAC is comprised of 28 senior executives representing major carriers, information systems providers, manufacturers, electronics firms, and aerospace firms."[28]

This is one of the single most important groups created to advise the President. The major industry leaders and corporate CEO's of the civilian sector have a mechanism to ensure their collective voices are heard on matters that deal with their industries as they relate to programs and initiatives proposed by the government regulating agencies and the Congress. As previously indicated, the tremendous dependence on the Public Switched Network (PSN) has forced this consortium of government and private sector leaders to resolve infrastructure incompatibilities in a joint forum. Some of the activities and issues previously addressed by this group include,

> "Assured Access, Physical Security, Industry Information Security, Telecommunications Systems Survivability, Automated Information Processing, Commercial Network Survivability, Commercial Satellite Survivability, and Dual Use Applications."[29]

With the enumerable committees and boards which have been

established to examine defensive capabilities and requirements, there has been little effort to appoint or assign a department or agency with the responsibility for implementation of defenses. Since the nature of an attack against the national information infrastructure would be a disaster that would affect major areas of the United States, why isn't the Federal Emergency Management Agency (FEMA) in charge of these defensive efforts? After all, their mission of directing and coordinating the nations emergency assets during times of natural disaster or national calamity most surely places them in the role of major contributor to the effort. W. Oscar Round and Earle L. Rudolph, Jr., in their article on "Civil Defense in the Information Age," suggest, "Assignment of a lead agency with adequate capability to meet the security demands posed by the evolving techno-threats would be a first step in building a viable federal response [to information warfare attacks]."[30] In a related article in Defense News, Rudolph goes on to say, "Someone has to be the leader, to assign roles and exercise direction. FEMA has the national security links."[31] As a counter argument to this proposal, retired Vice Admiral Jerry Tuttle, vice-president of Oracle Corporation explains,

> "FEMA is an organization that responds to catastrophes, and does not have the culture needed to take proactive steps to safeguard the infrastructure....For that reason, FEMA would not make the best lead agency to protect cyberspace, which should be handled by a hybrid organization composed of Pentagon and industry leaders."[32]

If the Federal Emergency Management Agency is not the answer, as

Tuttle asserts, is there a government agency that should be assigned this responsibility? And if a government department or agency is assigned, will the assignment be acceptable to the private sector? The National Information Infrastructure has become so interwoven with governmental and private sector participants that some worry whether or not the government may try and impose requirements on the establishment and maintenance of the National Information Infrastructure. Congressional sources attempt to mitigate this implication stating,

> "The whole idea is that all government and private sector communications are working together....The government obviously doesn't have a right to mandate how these systems are setup and [to] have control over these systems. But there's a federal interest involved."[33]

A tricky balancing act will have to be performed as future requirements may demand decisions that subordinate the rights of private citizens and corporations to those of the collective national interests. Other measures being entertained by the Congress include an amendment to the Senate's version of the current (FY96) Defense Authorization Bill.

> "Introduced by Sens. John Kyl (R-Ariz), Charles Robb (D-Va), and Jeff Bingaman (D-N.M.)...[t]he amendment would require the White House to outline procedures for how all major U.S. communications systems would perceive, assess, and warn of attacks from foreign nations or groups."[34]

> "Specifically, the bill calls on the president to submit to Congress a report setting forth 'the national policy and architecture governing the plans for establishing procedures, capabilities, systems and processes necessary to perform indications, warning and assessment functions regarding strategic attacks by foreign nations, groups or individuals or any other entity against the National Information

> Infrastructure.'...The Security Policy Board has suggested creating a new policy-making body called the Information Systems Security Committee [ISSC]. Reporting to the NSC, the ISSC would set information security policy for civilian, Defense and intelligence agencies."[35]

## Conclusions

Unfortunately, there is no national definition, strategy, or policy that can provide overarching guidance for defensive or offensive information warfare concerns. Differences in definition, as well as a focus on individual needs, seem to preclude development of a unified effort without the definitive guidance that a stated national policy might provide.

It is obvious that the gravity of the information security issues are recognized within Congress. Efforts to enact meaningful legislation are on-going. Calls for studies and reports can only increase our knowledge of the complexities associated with information systems security. The Department of Defense, the National Security Agency, the Office of Management and Budget, the Department of Commerce, the National Institute of Standards and Technology, The Government Services Agency, the Central Intelligence Agency, the Federal Emergency Management Agency, the Joint Security Commission, the Security Policy Board, the Security Policy Advisory Board, and the National Security Telecommunications Advisory Committee, as well as members of Congress and the Office of Technology Assessment are all working on these concerns. While there may be some overlap between participants, there appears to be much fragmentation and a lack of a coherent integrated plan.

To achieve a necessary unified focus, a coherent national policy for the security of our national information systems is necessary. This policy should define what constitutes an attack on our vital national interests and the appropriate response to such an attack. The policy would further add to the current choices of flexible deterrent options available to the President during any crisis analysis and course of action development. Without benefit of an overarching and cohesive national policy on information warfare, we cannot derive a definition or a concept upon which to base an intended strategy. Committees such as the Security Policy Board, the National Security Telecommunications Advisory Committee and the Information Systems Security Committee have the requisite composition of government and private industry leaders to serve as a pool from which to establish a single authority to implement such a policy. This policy would then serve as the zenith for our fragmented efforts and bring them together in a complementary program. Absent strong emphasis from the Executive Branch and without an authoritative body to direct these multiple fragmented efforts into a complementary program, our abilities to carry out any strategy are severely degraded. If it seems to be asking the impossible, then so be it. Many times in the history of warfare, the impossible has been asked and achieved.

ENDNOTES

1. Carl von Clausewitz, On War, ed. & trans. by Michael Howard and Peter Paret. (Princeton: Princeton University Press, 1976), 595-596.

2. Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Information Warfare briefing. (Washington: Department of Defense, 1994) slide 2.

3. Ronald R. Fogelman, "Information Operations: The Fifth Dimension of Warfare," Defense Issues Vol. 10, No. 47, 1995, 1.

4. Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, (Washington: Science Applications International Corporation (SAIC) Contract No. MDA903-93-D-0019, 4 July 1995), 1-1.

5. As quoted by, Alvin and Heidi Toffler, War and Anti-war (New York: Warner Books, Inc. 1993), 175.

6. Alan D. Campden, "Rush to Information-Based Warfare Gambles with National Security," Signal (July 1995): 68.

7. Douglas Waller, "Cyber Soldiers," Time, 21 August 1995, 44.

8. Department of Defense, "Assessing Network Vulnerabilities," (Washington: Defense Information Systems Agency briefing, 1995), slide 20.

9. Waller, 44.

10. Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 1-1.

11. Campden, 68.

12. William V. Roth, "Information Security and Privacy on Computer Networks," (Washington: U.S. Senate prepared statement, released September 23, 1994.

13. Ibid.

14. Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-14, 2-33, 2-34, 2-36, 2-39, 2-40.

15. An extract from, John Perry Barlow, "A Cyberspace Declaration of Independence," electronic mail bulletin board (www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296.declaration), 9 FEB 96. The entire piece can be found at this address.

16. Y. Harkabi, "Nuclear War and Nuclear Peace," Military Strategy: Theory and Application, (Carlisle Barracks (PA): U.S. Army War College, 1993), 274.

17. Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Information Warfare briefing, (Washington: Department of Defense, 1995), slide 13.

18. Daniel E. Magsig, "Information Warfare in the Information Age," (Course Hand-out for USAWC Advance Course 567cj, U.S. Army War College, 1995), 3.

19. National Defense University, "School of Information Warfare and Strategy; A working dictionary," (Washington: National Defense University, Academic Year 1994-95), 31.

20. Department of the Army, Information Operations, FM 100-6, (Washington: U.S. Department of the Army (Drag Draft), 2 OCT 1995), Glossary-11.

21. A National Security Strategy of Engagement and Enlargement (Washington: The White House, February 1995), 8.

22. National Military Strategy of the United States of America (Washington: U.S. Department of Defense, 1995), 15.

23. Department of the Army, Information Operations, FM 100-6, i.

24. Department of Defense, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-19,2-20,2-53.

25. Ibid., 2-53,2-54.

26. Ibid., 2-8.

27. Ibid., 2-9.

28. Fact Sheet, "The President's National Security Telecommunications Advisory Committee (NSTAC)," (Washington: n.p., 23 February 1996).

29. Ibid.

30. W. Oscar Round and Earle L. Rudolph, Jr., "Civil Defense in the Information Age," Strategic Forum, No. 46, September 1995, 3.

31. Pat Cooper and Robert Holzer, "America Lacks Reaction Plan for Info War," Defense News, October 2-8, 1995, 3&37.

32. Ibid.

33. Ibid.

34. Elizabeth Sikorovsky, "Bill directs White House to design plan," Federal Computer Week, Vol. 9, No. 23, August 14, 1995, 8.

35. Ibid., 14.

BIBLIOGRAPHY

Arquilla, John and David Ronfeldt, "Cyberwar is Coming," Santa Monica: Rand Corporation, 1992.

Barlow, John Perry. An extract from "A Cyberspace Declaration of Independence," electronic mail bulletin board(www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296.declaration), 9 February 1996.

Campden, Alan D. "Rush to Information-Based Warfare Gambling with National Security," Signal, July 1995, 68.

Clausewitz, Carl von. On War. Edited and Translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1989.

Cooper, Pat and Robert Holzer, "America Lacks Reaction Plan for Info War," Defense News, October 2-8, 1995.

Defense Information Systems Agency. "Assessing Network Vulnerabilities," Washington: Defense Information Systems Agency briefing, 1995.

Fact Sheet, "The President's National Security Telecommunications Advisory Committee (NSTAC)," Washington: n.p., 23 February 1996.

Fogelman, Ronald R. "Information Operations: The Fifth Dimension of Warfare," Defense Issues, Vol. 10, No. 47, 1995.

Harkabi, Y. "Nuclear War and Nuclear Peace," Military Strategy: Theory and Application, Carlisle Barracks, PA: U.S. Army War College, 1993, 274.

Holmes, W.J. Double-Edged Secrets: U.S. Naval Intelligence Operations in the Pacific during World War II. Annapolis: Naval Institute Press, 1979.

Libicki, Martin C. The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon. Washington: Institute for National Strategic Studies, National Defense University, 1995.

Magsig, Daniel E. "Information Warfare in the Information Age," (Course hand-out for USAWC Advance Course 567cj, U.S. Army War College, 1995, 3.

National Defense University, "School of Information Warfare and Strategy; A Working Dictionary," Washington: National Defense University, Academic Year 1994-95, 31.

Office of the Chairman of the Joint Chiefs of Staff, National Military Strategy of the United States of America, Washington: U.S. Department of Defense, 1995.

Office of the President of the United States, A National Security Strategy of Engagement and Enlargement, Washington: The White House, February 1995.

Roth, William V. "Information Security and Privacy on Computer Networks," Washington: U.S. Senate prepared statement released September 23, 1994.

Round, Oscar W. and Earle L. Rudolph, Jr. "Civil Defense in the Information Age," Strategic Forum, No. 46, September 1995.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Super-highway. New York: Thunder Mouth Press, 1994.

Sikorovsky, Elizabeth, "Bill directs White House to design plan," Federal Computer Week, Vol. 9, No. 23, August 14, 1995.

Stiz, Gary. "Fighting Future Wars," Scientific American, December 1995.

Toffler, Alvin and Heide, War and Anti-war. Boston: Little, Brown, 1993.

U.S. Congress, Office of Technology Assessment, "Information Security and Privacy in Network Environments," Washington: U.S. Congress, Office of Technology Assessment, 1994.

U.S. Department of the Army, Information Operations, FM 100-6, Washington: U.S. Department of the Army (Drag Draft), 2 October 1995, Glossary-11.

U.S. Department of Defense. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. Washington: U.S. Department of Defense, 1995.

U.S. Department of Defense, Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Information Warfare briefing, Washington: U.S. Department of Defense, 1994.

U.S. National Defense University. Strategic Assessment 1995: U.S. Security Challenges in Transition. Washington: Institute for National Strategic Studies, National Defense University, 1995.

Waller, Douglas. "Cyber Soldiers," Time, 21 August 1995, 44.